International Journal of Computer Science Engineering
and Information Technology Research (IJCSEITR)
ISSN (P): 2249-6831; ISSN (E): 2249-7943
Vol. 9, Issue 2, Dec 2019, 29-36

THE DESIGN AND DEVELOPEMENT OF DECENTRALIZED DIGILOCKER USING BLOCKCHAIN

AMRITA B. CHAVAN & Dr. K. RAJESWARI

Department of Computer Engineering, Pimpri Chinchwad College of Engineering, Nigdi, Pune, India

ABSTRACT

Document storehouse with compact services is weak against information breaches and alike precise denial of service, in the event that the service is destroyed. Clients have no control on a chamber compelling the service to open their information. The reports are powerless against theft from insiders fit for getting the encryption keys. By using blockchain technology on ethereum platform a decentralized digital locker able to work in server less fashion as decentralized applications (Dapp). It permits the clients to transfer and store individual records, which are encoded and saved in a decentralized way utilizing amenities. For Ex, Inter Planetary File System (IPFS). This file system is a showcase of ethereum Dapps, where the encryption keys are prolonged and open just to the end client. The client can also share the reports safely with various clients that they pick. Also the ID document will be stored in the hash format. The solidity smart contracts help to make tamper-proof records. It provides animmutability.

KEYWORDS: Blockchain, Dapps (Decentralized Applications), Ganache Server, Truffle Framework, IPFS, Metamask, Decentralization & Ethereum

Received: May 14, 2019; **Accepted**: Jun 05, 2019; **Published**: Jun 27, 2019; **Paper Id.**: IJCSEITRDEC20195

Original Article

INTRODUCTION

A change in outlook in the manner in which software models is drawing nearer. When cryptographic money like Bitcoin, influenced us to rethink about the meaning of Store of Value (SoV), it uncovered a private look of things to come: nowadays, a world running on decentralized applica- tions (Dapps). These adaptable, resourceful, straightforward and boosted applications will justify themselves to the world. The boom in technological advancement has led to the rapid rise in the development of digital asset transactions. One of the major technological advancements in the field of digital technology is the advent of the decentralized Blockchain technology. The Blockchain development technology offers the ease of storing and accessing data in a decentralized manner [15]. For large-scale use, the Digilocker could be an effective solution. The digital locker (Digilocker) is a document storage, verification and utility service that was launched by the government under the Digital India initiative. The intent was to eliminate the need for providing original and physical identity related or other important documents for an individual verification, and move to a technology- enabled and secure digital environment [16]. Before we can even appreciate what Dapps do, we have to know about its basic technology the blockchain. A blockchain is a ledger of records sorted out in ’blocks’ that are connected together by cryptographic approval. It is a digital cache of reconciliation truth. The key is to comprehend that this ledger is neither stored in a unified area nor overseen by any single element. The square approval framework results in new transactions being included irreversibly and old transactions saved always for all to see, consequently its purity and flexibility [7]. Open- source software that use on the blockchain technology are called Dapps. There are apparent normal highlights of Dapps: Open Source. Rather, it

essential to be represented via self- rule and all progressions must be chosen by the dominant part, of its clients. Its code base required to be accessible for examination.

- **Decentralized:** All records of the application's activity must be stored on an open and decentralized blockchain to stay far from involvement of centralization.
- **Boosted:** Validators of the blockchain must be boosted by balancing the mlike wise with cryptographic tokens.
- **Convention:** The application network must admit to a cryptographic calculation to demonstrate proof of value. For instance, Bitcoin utilizes Proof of Work (PoW) and ethereum is as of now utilizing PoW with plans for a cross breed Po W/Proof of Stake (PoS) later on.

The first Dapp was in reality Bitcoin itself. Bitcoin is an actualized blockchain arrangement that arrive from issues rotating around centralization and oversight. One can say Bitcoin is a self-continuing open ledger that permits effective transactions without middle people and brought together specialists. While both Bitcoin and Ethereum might be approximately character- ized as Dapps gone for taking care of true issues, Ethereum has an a lot greater arrangement at the top of the priority list The aim of Ethereum is to make an elective convention for building decentralized applications with accentuation on improvement time, security, and scaling[6]. You may consider Ethereum, for the absence of a superior similarity, the Mother of Dapps. Outfitted with its own one of a kind dialect, Solidity, Ethereum empowers designers to shape keen contacts utilizing the Turing-finish Ethereum Virtual Machine (EVM). With these instruments accessible, engineers made Dapps that have genuine use cases.

REVIEW OFLITERATURE

When document is store at central server then it is vulnerable to data breaches and may even lead to denial of service. Users have no control on a government forcing the service to disclose their data. The documents are unsafe from insiders. In this paper the prototype has been built of using Ethereum Dapps, where the encryption keys are maintained and accessible only to the end user on their device. The user can also share the documents securely with other users that they choose. An Ethereum smart-contract facilitates this transfer and creates a verifiable audit trail of the same Maintaining the Integrity of the Specifications [1].

One of the first successful utilization of blockchains ability to provide encrypted, peer-to-peer model of decentralized trans- action recording was within the financial sector. Bitcoins, the now famous type of crypto-currency, was developed based on the blockchain technology back in 2008. It has collect a strong interest from the best of financial institutions. Blockchain may enable companies such as JP Morgan Chase, Citigroup, and Credit Suisse, all of which are currently investing in the technology, to do more with less, streamline their businesses and reduce risk in the process[2].

Blockchain technology stores data in a decentralized, trusted and immutable manner. Blockchains can ensure that the user's single digital identity is stored in a secure and incorruptible manner. This single digital identity can always be up-to-date with the latest user information. Civic, which focuses on fraud reduction and protection from identity theft, had an extremely successful ICO last July [3].

The blockchain is a new technology that provides (almost)free for-all ledger records of all transactions within its boundaries. It is also a transfer system in which parties can send, receive, and keep digital coins for a variety of reasons. Thus, it is important to understand that crypto currencies are just sphere of the blockchain, which holds a lot more

applications in the real world, not just holding coins of value. Apart from transactions, any sort of information can be recorded. Any of the records cannot be changed on the latter date, as to provide complete transparency. The main goal of blockchain technology is to provide a completely decentralized environment, where participants of the system create and maintain the network. The database is equally available to all individuals, regardless of their background and wealth[4].

Most online transactions require that individuals disclose specific personal information before they can proceed to access services. For instance, before financial transactions can be carried out on platforms such as Amazon Pay, PayPal and Google Wallet, among others, users are always required to input their sign up/login details i. e., financial and personal details. Thus, every time an individual discloses this information, it gets stored on numerous internet databases. As such, digital clones of one and the same individual spring into existence across these different platforms. This also exposes a lot of security issues. Thus, as evidenced by the Equifax hack, gaining access to a major data base exposes all the personal information of users and exemplifies the high vulnerability of the current system. Most systems in place rely heavily on obtaining individual data without the knowledge of the owner, and third parties can, in turn, gain access to this data without the subjects knowledge [5]. In light of which blockchains how these DApps use, they are characterized into three classes Several current applications are based over these categories.

- **Type 1:** These types of Dapps have their own blockchain (like bitcoin). Other altcoins also fall under this category as well.
- **Type 2:** These types of Dapps use the blockchain of Type I Dapps. Decentralized applications are protocols and have tokens that are necessary for their function. The Omni Protocol is an example of Type 2 decentralized application.
- **Type 3:** These types of Dapps use the protocol of a Type 2 Dapp. For example, the SAFE network uses the Omni Protocol for issuing Safe Coins that are then used to build distributed file storage[18]

SYSTEM ARCHITECTURE / SYSTEM OVERVIEW

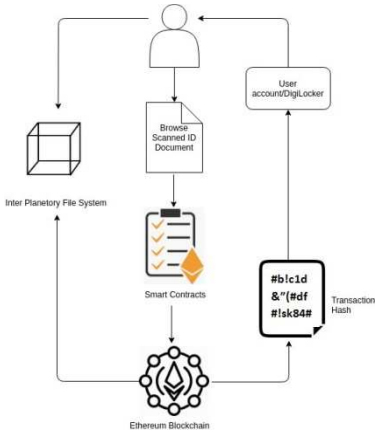

Figure 1: System Architecture

A decentralized digital locker can be built in a server-less fashion (as a Dapp) by leveraging Ethereums blockchain technology. It allows users to upload and store personal documents that are encrypted and stored in a decentralized manner. The user can also share the documents securely with other users that they choose. An Ethereum smart-contract facilitates this transfer and creates a verifiable audit trail of the same.

Digilocker Decentralized application structure is composed by a front-end interface (Web Browser, HTML, CSS) and a back-end interface (Web3 JavaScript). As described in the figure below, the Dapp application interacts with the Ethereum node (EVM) using JSON RPC. JSON RPC is a stateless and lightweight remote procedure call (RPC) protocol that is used by Ethereum clients to interact with an Ethereum node[1].

PROPOSED METHODOLOGY

The Digital Locker application communicates a work pro- cess of sharing digitally bolted records where the owner of the documents controls the entrance to these documents. We outline Digital Locker utilizing a case of an owner performing access control to their report held by a bank. The state transition diagram underneath demonstrates the collaborations among the states in this work.[6] An occasion of the Digital Locker application's work process begins in the Requested state when an Owner asks for their bank to start a procedure of sharing a record held by the bank. A Bank Agent makes the state transition to Document Review by calling the capacity Begin Review Process demonstrating that the procedure to audit the demand has started. When the audit is finished, the Bank- Agent at that point makes the report available by transferring the records. The Available To Share state can be thought of a ceaseless state, more on this in a bit. When the report is available to share, the record can be shared either with an outsider that the owner hosts distinguished or any arbitrary third-get-together requestor

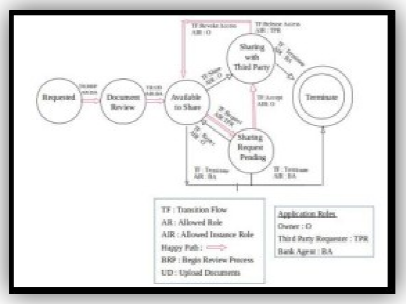

Figure 2: Digi Locker State Transition

In the event that the owner determines the outsider requestor, the state transitions from Available to Share to Sharing with Third Party. On the off chance that an irregular outsider requestor needs access to the report, that outsider requestor first demands access to the record. Now, the owner can either acknowledge the demand and allow access or reject the demand. On the off chance that the owner rejects the demand to the irregular outsider requestor, the state returns to Available to Share. On the off chance that the owner acknowledges the demand to permit the arbitrary outsider demand to get to the archive, at that point the state transitions to Sharing with Third Party. When the outsider requestor is finished with the archive, they can discharge the bolt to the report and the state transitions to Available To Share. The owner can likewise make the state transition from Sharing with Third Party to Available To Share when they deny access from the outsider requestor. At long last, whenever amid these transitions the bank specialist can choose to end the sharing of the archive once the record winds up available to share [6]. The below code snippet gives the main function of sharing documents and working pattern and states are described above. Function ShareWithThirdParty (address third Party Requestor, string expiration Date, string intended Purpose)

```
if (Owner != msg.sender)
```

revert();

Third Party Requestor = third Party Requestor;

Current Authorized User = Third Party Requestor;

Locker Status =”Shared”;

Intended Purpose = intended Purpose;

Expiration Date = expiration Date;

State = State Type. Sharing With Third Party; Contract Updated (”Share with Third Party”);

In this system, we are making tamper-proof transactions by applying smart contracts on them. So it’ll overcome the theft of ID proofs or any confidential document and store it in our DigiLocker. One more advantage of this system is minimal or only required information will be disclose from our document, nobody can hack it.

RESULTS AND DISSCUSSIONS

Data Set: Real world documents like land contracts, Aadhar Card, Driving Licence, Voter ID etc of some 100 people.

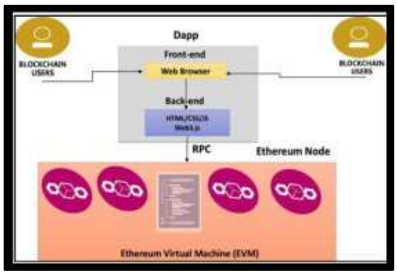

Figure 3: Working of Dapp

Digilocker Dapp Performance and Transaction Status

Firstly we will compile our solidity smart contract which is the basis of transaction between two accounts. Meta Mask is a bridge that allows you to visit the distributed web of tomorrow in your browser today. It allows you to run Ethereumd Apps right in your browser without running a full Ethereum node. Meta Mask includes a secure identity vault, providing a user interface to manage your identities on different sites and sign blockchain transactions. Meta mask is used to choose ropsten test network and show the interaction between accounts below figure shows the contract deployment status: Contract is deployed from 0x7f1be5223136751111167d1b57c67eccd08976ba account address to 0x83207c910b6af6a56ce0df9ef8b3278f8175d187 and the whole transaction summary i. e. its success can be seen in below figure:

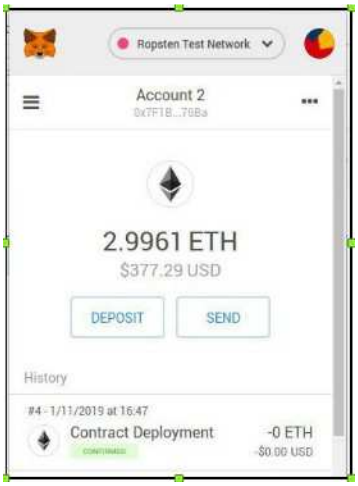

Figure 4: Contract Deployment on Metamask

Figure 5: Transaction Successful

Our block status gas price and other statistics can be seen in below ethers can window:

Figure 6: Statistics

CONCLUSIONS

Our demonstration shows a practical implementation of a DAPP for sharing objects. This study is conducted with the ultimate aim to make a Decentralized Dapp on which user must have their own control on their documents. This experiment is conducted using Smart contracts in solidity, Remix IDE, Ganache Server, Metamask (Ethereum based Dapp), React JS(Frontend), and IPFS(Inter Planetory File System). The Blockchain technology plays very important role to make our Identity decentralized. This Dapp is useful to secure our documents and can store it into hash format so that no one hack it we implement a sharing solution for power tools. In our smart contract demonstration, we have an owner add a document to the web app, have an additional person ask the access, and then return or reject the document thereafter; thus presenting the four core functions of our smart contract.

FUTURE WORK

Newer Decentralized Identity can be proposed by modifying the layers in this model to have better results like:

- when we'll be click on hash value then control will directly goes on IPFS and we can see our original document

- By using this Dapp we'll be able to share the hash value with other organization like college, office, bank for document verification.

REFERENCES

1. *Blockchain: Decentralized Digital Locker — Persistent Systems. Ac- cessed January 31, 2019. https://www.persistent.com/new-and-emerging- tech/blockchain/digital-locker-dapp/*
2. *Building Decentralized Applications - Dapps - on Blockchain — LinkedIn. Accessed February 1, 2019. https://www.linkedin.com/pulse/building- decentralized-applications- dapps-blockchain-kamat/.*
3. *Industries EBloque. Accessed February 1, 2019. http://www.ebloque.com/industries/.*
4. *Jurowiec, Piotr. This Thing Called Blockchain. [Beginners Guide]. PiotrJurowiec (blog), August 20, 2018. https://medium.com/@piotr- 61543/this-thing-called-blockchain-beginners-guide-1849d79f1c99*
5. *How Blockchain Can Solve Identity Management Problems. Accessed February 1, 2019. https://www.forbes.com/sites/forbestechcouncil/201 8/07/27/how-blockchain-can-solve-identity- management-problems/2436b8e813f5*
6. *Azure Blockchain Content and Samples. Contribute to Azure- Samples/Blockchain Development by Creating an Account on GitHub. HTML. 2018. Reprint, Azure Samples, 2019. https://github.com/Azure- Samples/blockchain.*
7. *Bogner, Andreas, Mathieu Chanson, and Arne Meeuw. A Decentralised Sharing App Running a Smart Contract on the Ethereum Blockchain. In Proceedings of the 6th International Conference on the Internet of Things - IoT16, 17778. Stuttgart, Germany: ACM Press, 2016. https://doi.org/10.1145/2991561.2998465.*
8. *Blockchain and Digital Identity A Good Fit? Internet Society (blog), March 13, 2018. https://www.internetsociety.org/blog/2018/03/blockchain-digital-identity-good-fit/*
9. *ahammad, raju. Aivon Artificial Intelligence Image Identifier. Raju Ahammad (blog), November 30, 2018. https://medium.com/@rajuahammad1981/aivon- artificial-intelligence- image-identifier-3371250080e5*
10. *Decentralized Digital Locker Blockchainerz. Accessed Febru- ary 27, 2019 https://articles.abilogic.com/310377/decentralized-digital- locker-blockchainerz.html*
11. *Digital Identity Management for NGOs Using Blockchain (Hack Society 2018 Entry). Dynaquest (blog), October 22, 2018. http://www.dqtsi.com/2018/10/22/digital-identity- management-for-ngos- using-blockchain-hacksociety-2018-entry/.*
12. *How Blockchain Can Solve Identity Management Problems - One Kosmos (BlockID). Accessed February 1, 2019. https://onekosmos.com/blog/how-blockchain-can-solve-identity-management-problems/*
13. *What Is DApps (Decentralised Apps)? BTC Wires (blog). Ac- cessed February 1, 2019. https://www.btcwires.com/glossary/what-is-dapps-decentralised-apps/*
14. *South African Crypto currency Magazine. Crypto currency Yes or Now - Read More Here! Accessed February 1, 2019. http://technomagazine.net/image-post46.html.*
15. *Digital Transaction Limited. Accessed February 1, 2019. http://www.digital-transaction.com/en-protect-identity.php.*

16. *Jaju, Amit. Demystifying the Potential of a Digilocker. https://www.livemint.com, October 2, 2017.*

    https://www.livemint.com/Money/paRe9z8I3K53MjvLSXGtkJ/Demystifying- the-potential-of-a-Digilocker.html

17. *Step by Step Guide to Build a Dapp. Heptagon (blog), Paul, Moses Sam. March 8, 2018.*

    https://medium.com/heptagon/step-by-step-guide- to-build-a-dapp-a-homo-sapiens-2-day-love-affair-with-ethereum-dapp-de2b0dea12f1

18. *What Are DApps (Decentralized Applications)? The Beginners Guide. Coin Sutra - Bitcoin Community, July 24, 2017.*

    https://coinsutra.com/dapps-decentralized-applications

19. *Al-Azhari, W. W. Landscape Learning; Xeriscaping Design techniques: The Case of Jordan University.*

20. *haskar, Abhijirt. Keep Your Aadhaar, Other Docs Safe. Shift to DigiLocker App*

    https://www.livemint.com, December 21, 2018

    https://www.livemint.com/Technology/B8y8bQgQxob9WW8EreG2mK/Keep-your-Aadhaar-other-docs-safe-Shift-to-DigiLocker-app.html

21. *ames. The Basics of Decentralized Identity. UPort (blog), June 27, 2018.*

    https://medium.com/uport/the-basics-of-decentralized-identity- d1ff01f15df1